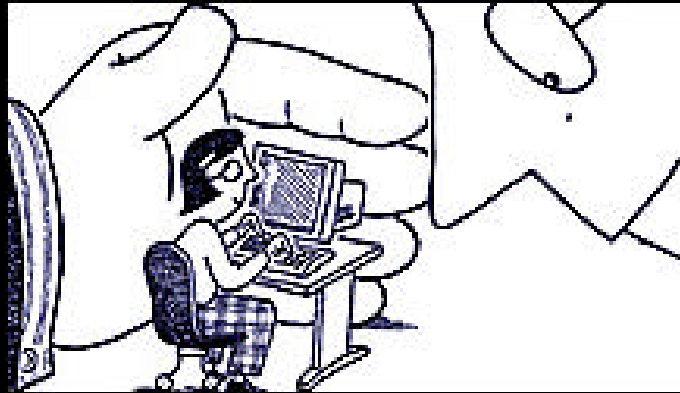


TEACHING COMPUTERS TO FORGET



Michael A. Caloyannides, PhD

Mitretek Systems

micky@IEEE.org

Why the concern ?

- ✍ Computers have replaced a lot of paper.
- ✍ We entrust computers with material that, in the past, we would never have committed to paper.
 - ✍ The proliferation of email.
 - ✍ Treated as water fountain gossip.
 - ✍ But it is extremely permanent.
- ✍ Computer forensics is done because it CAN be done cheaply and pays off.

Why should you care?

- ✧ As an employee
- ✧ As an employer
- ✧ As an individual PC user at home
- ✧ As an insurance company
- ✧ As a user of others' computers
- ✧ As a medical professional
- ✧ As a businessman

- ✧ YOU CAN BE HELD LIABLE FOR NOT PROTECTING OR REMOVING SENSITIVE INFORMATION FROM YOUR COMPUTER

Most commercial products (e.g. Microsoft's) usually default to "everything enabled", (hence to "no security")

- ✍ It is up to each individual user of Windows and Microsoft application software to raise the security level of his/her setup.
- ✍ Unix flavors usually come with minimal security enabled "out of the box", too.

“If you have done nothing illegal, then you have nothing to fear”

Not true at all!

- a) Holocaust victims,
- b) posthumously exonerated executed persons, etc.

It is wise, therefore, to minimize the likelihood that anything in your computer, taken out of context, can be used against you.

"BUT THAT IS NOT MY FILE..."

- ✍ The German Chaos Club demo
 - ✍ (causing someone's "Quicken" to order funds to be transferred to the hackers' account)
- ✍ Unsolicited scantily clad underage images from pop-up ads while web-browsing. Read: JAIL
- ✍ BO/BO2K – like software opens the back door.
- ✍ The Used hard disk (or computer) can contain anything at all that can be used against you.
- ✍ etc., etc.

“BUT I DIDN’T DO THIS ONLINE...”

- Anyone can access your ISP through YOUR 802.11b:
 - ✍ What if someone sent a threatening email to the President from YOUR (wireless) online connection?
 - ✍ By the way, the problem is in the IV; longer encryption keys do not address the real security problem.
- Or you may access unintended sites through hijacked DNS:
 - ✍ Unintentional adult site browsing and caching on your disk
- etc., etc.

GOOD LUCK CONVINCING A
TECHNOLOGY-CHALLENGED
JURY THAT YOU DIDN'T DO IT.

(most defense lawyers are
uninformed about how to defend
cases based on computer
“evidence”)

"BUT I HAVE MY RIGHTS..."

- ✍ "CyberSLAPP" suits to silence corporate criticisms
 - ✍ Strategic Lawsuits Against Public Participation
- ✍ The Northwest Airlines case where HOME computers were subpoenaed in a civil matter
- ✍ The DMCA impact.
 - ✍ Security flaws go unpublished or even undiscovered. Certainly not fixed.
- ✍ A lawsuit, even if frivolous, can lead you into bankruptcy in defending from it.

PROTECT WHAT AND FROM WHOM?

The answer to this determines
what protective measures you
need to take.

See “**Desktop Witness**” book (John Wiley Co.)

A COMPUTER FILE YIELDS *MORE* EVIDENCE AGAINST YOU THAN PAPER FILES

- ✎ Shows data/time of creation.
- ✎ Shows data/time of last access.
- ✎ Shows whose serial-numbered copy of a word processor created it.
- ✎ Shows sequence of changes and dates.
- ✎ Shows which folders the file has been through?
- ✎ Shows if file was printed, where and when.

SO, YOU NOW WANT TO PROTECT *EXACTLY* WHAT?

- ✦ The **content** of a file?
- ✦ The **metadata** (data about the data) about the file?
- ✦ Protect **who** communicated with whom?
 - ✦ That connectivity can be damning in and by itself in some situations

Each of the above requires obviously different defenses.

PROTECTING THE CONTENT

- ✍ *“I will delete it”. Or “I will encrypt it”.*
- ✍ If only it were that simple...

So, exactly where is the evidence hiding?

- ✍ In far too many different places for even the experienced user to track.
- ✍ Some of these places cannot be *accessed* by even experienced users.
- ✍ Incinerating the data storage media may be the only way to get rid of some data.

[Exactly where can sensitive data be hiding?]

- ✂ “Deleted” files
- ✂ The “Slack”
- ✂ “Free space”
- ✂ Windows’ temp files
- ✂ Windows’ “Registry” entries
- ✂ Applications’ own history files
- ✂ Invisible portions of user-created documents and files
- ✂ SWAP file
- ✂ Hardware and software buffers
- ✂ Backup media
- ✂ Network facilities for those on a network
- ✂ **Mothballed sectors of high density HDs.**

[Exactly where is the evidence hiding?]

✍ The Microsoft “Allow Fast Saves” default option.

✍ ~~You wretched son of a~~ Dear Mr. Jones:

- ✍ What it does, why and how.
- ✍ British MOD got “burned” and so can you.
- ✍ Ditto for Excel.
- ✍ Ditto for “levels of undoing” in various software products (e.g. Adobe Photoshop, etc.).

PROTECT THE METADATA?

- ✍ Very hard to remove it or to alter it. It contains:
 - ✍ Date/time file was created.
 - ✍ Date/time file was last accessed.
 - ✍ Date/time file was moved to another folder.
 - ✍ *“This, your honor, proves that the accused knew...”*
 - ✍ *“Aha! So there used to be a removable drive F:”....*
 - ✍ Original name of file and new name(s).

PROTECT FROM WHOM?

- ✍ From the casual hotel maid?
 - ✍ Use a BIOS password, and file encryption.
- ✍ From the nosy neighbor?
 - ✍ Don't leave him/her alone with your computer.
- ✍ From one's enterprising son or daughter?
 - ✍ All bets are off.
- ✍ From the computer repairman you summoned?
 - ✍ Remove your hard disk and insert a bland one (they are inexpensive, so have one.)

(protect from):

- ✍ From a competent hacker?
- ✍ From adware/spyware?
- ✍ From a corrupt cop?
- ✍ From your estranged spouse's lawyer?
- ✍ From a business competitor?
- ✍ From an intelligence or secret police organization when traveling abroad?

(protect from)

- ✍ From your local ISP who sees all?
 - ✍ Use SSL
 - ✍ Dial another ISP, preferably out-of-country.
 - ✍ Use a satellite phone to another country's ISP.
 - ✍ Use a foreign-registered GSM cellphone.
- ✍ From a disgruntled employee of yours?
- ✍ From a telephone tap?

(protect from)

- ✍ From the search-engine company (e.g. google) that you have used?
- ✍ Search engines' source of revenue is:
 - ✍ The marketing value of your searching habits
 - ✍ The annoying pop-up ads
 - ✍ Being paid to steer you first to vendors who paid the most.
- ✍ Connect through anonymizing proxies and disable all cookies and scripts.

(protect from)

- ✍ From the in-country “anonymizing” service you have used, whose records have been subpoenaed?
 - ✍ Don’t use in-country anonymizers.
 - ✍ Avoid politically allied anonymizers, too.
- ✍ From an untrusted recipient of your “eyes only” email? Good luck !
 - ✍ The “Disappearing Email” ILLUSION. Readily defeatable.

(protect from)

✍ From **Microsoft's** snooping?

- ✍ Media Player uploads to MS the list of CDs/DVDs you play along with an ID for you.
- ✍ “Passport Terms of Use” (now watered down)
 - ✍ “By engaging in any form of communication through the Passport Web Site... you are granting Microsoft permission to ...”

(protect from)

From Netscape's snooping:

- ✍ “Search” function uploads data to Netscape.
- ✍ “What is related” does likewise.
- ✍ “Smart update”, “smart browsing” do likewise.
- ✍ Do NOT search from Netscape; go to a search engine instead.
- ✍ Disable “what is related”, “smart update” and “smart browsing”. Nothing smart about them.

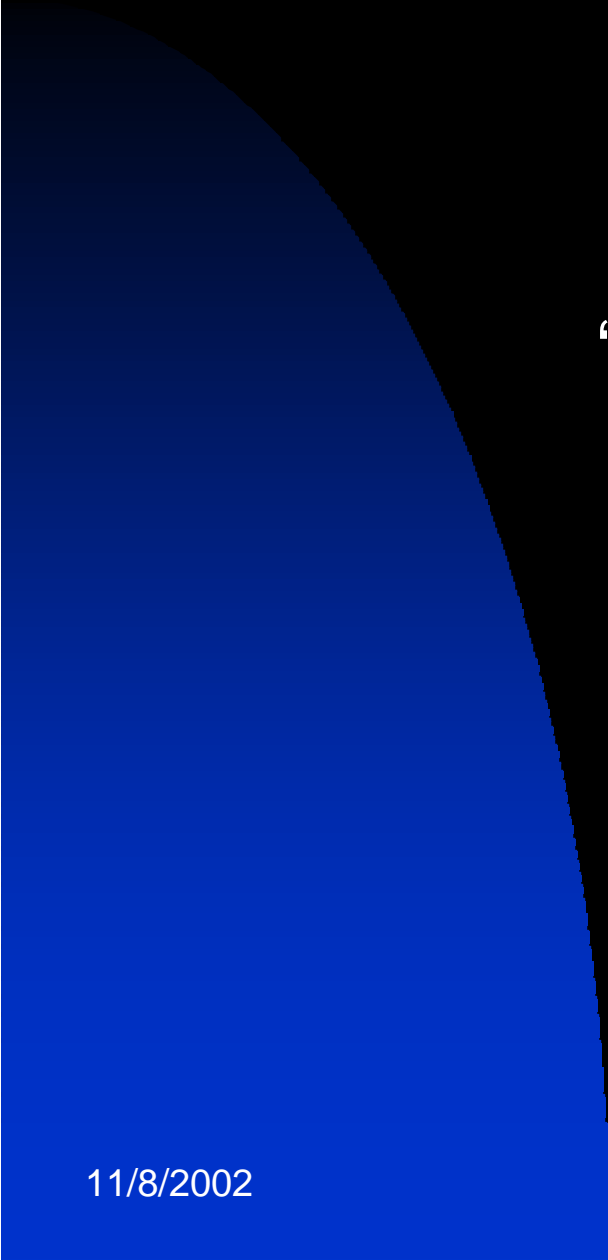
(protect from)

And on and on and on...

- ✍ Prodigy's shenanigans in years past and the California District Attorney's threat to prosecute.
- ✍ "The Wire"
- ✍ etc.

And speaking of browsers...

EVIDENCE LURKING IN BROWSERS

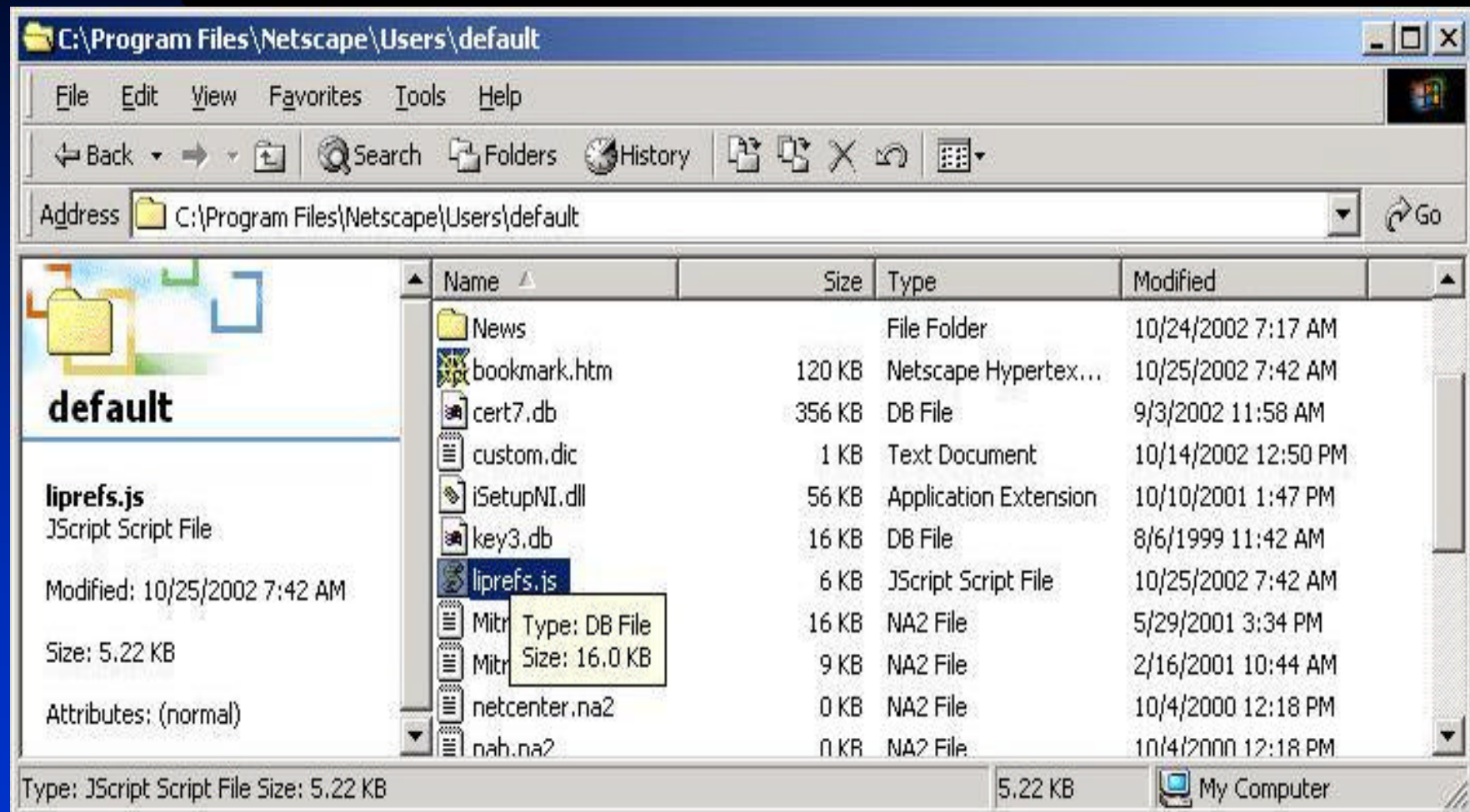


“...but I was only looking...
I didn't do anything...”

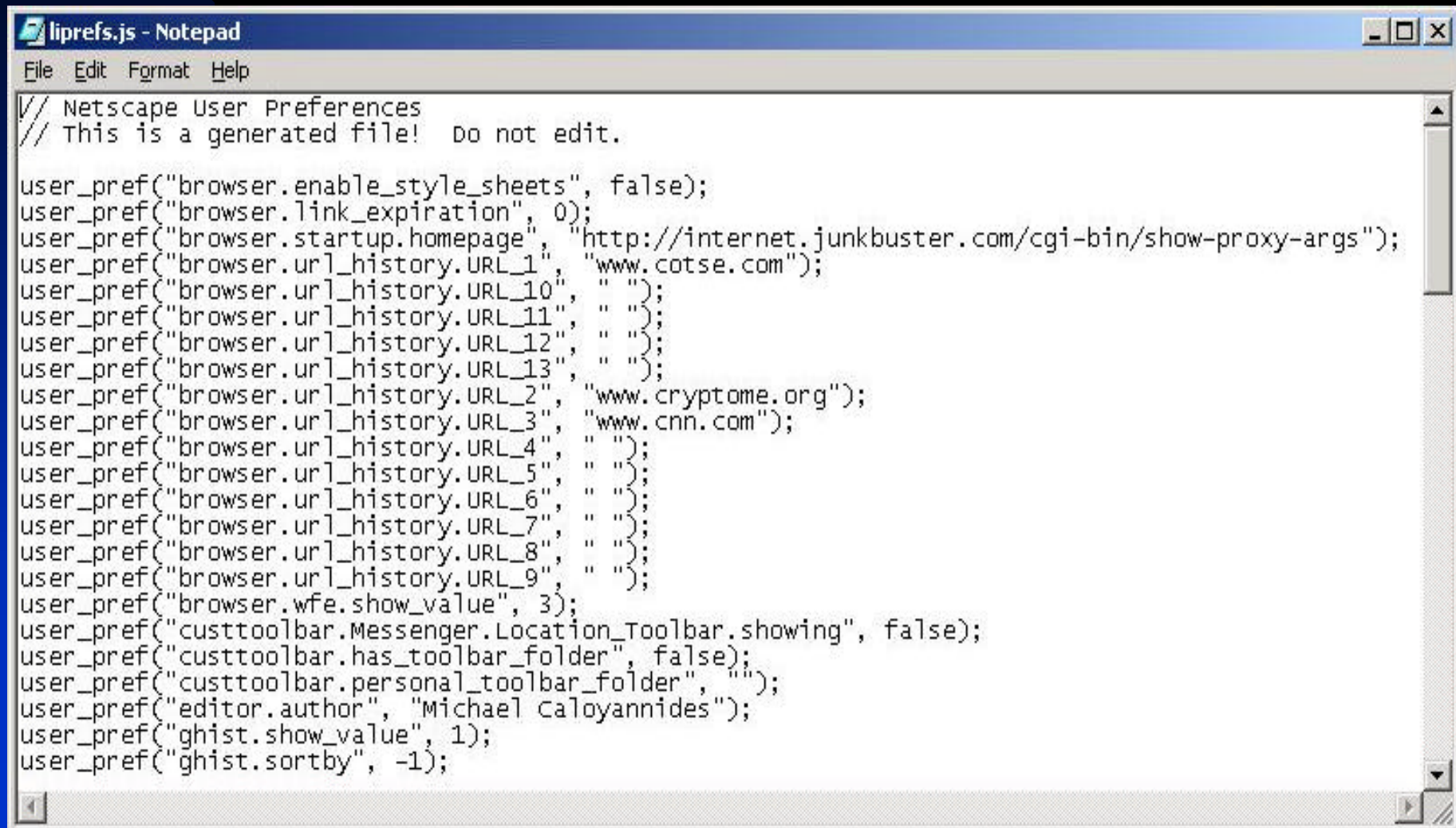
THE FACTS OF LIFE

- ✍ Web browsing is NOT passive at all.
 - ✍ You actively ask for and receive content.
 - ✍ You also receive and store content that you never asked for, such as images whose presence in your hard disk is now illegal.
 - ✍ And all this is recorded in your computer, and can also be recorded by your ISP, by police, and by the web sites you patronized intentionally or unintentionally.

LIPREFS.JS



AFTER BROWISING AT THREE WEB SITES

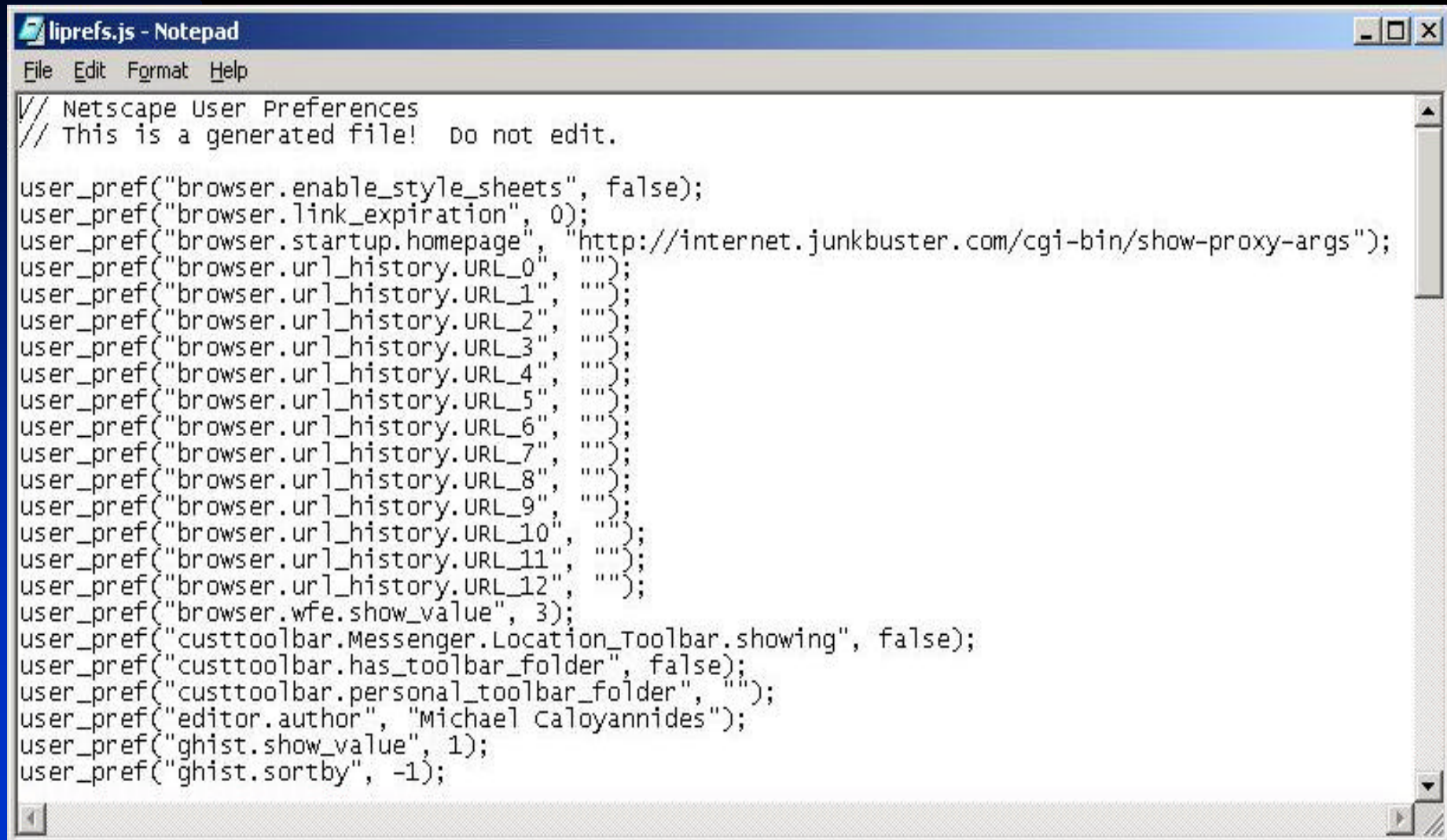


```
liprefs.js - Notepad
File Edit Format Help
// Netscape User Preferences
// This is a generated file! Do not edit.

user_pref("browser.enable_style_sheets", false);
user_pref("browser.link_expiration", 0);
user_pref("browser.startup.homepage", "http://internet.junkbuster.com/cgi-bin/show-proxy-args");
user_pref("browser.url_history.URL_1", "www.cotse.com");
user_pref("browser.url_history.URL_10", "");
user_pref("browser.url_history.URL_11", "");
user_pref("browser.url_history.URL_12", "");
user_pref("browser.url_history.URL_13", "");
user_pref("browser.url_history.URL_2", "www.cryptome.org");
user_pref("browser.url_history.URL_3", "www.cnn.com");
user_pref("browser.url_history.URL_4", "");
user_pref("browser.url_history.URL_5", "");
user_pref("browser.url_history.URL_6", "");
user_pref("browser.url_history.URL_7", "");
user_pref("browser.url_history.URL_8", "");
user_pref("browser.url_history.URL_9", "");
user_pref("browser.wfe.show_value", 3);
user_pref("custtoolbar.Messenger.Location_Toolbar.showing", false);
user_pref("custtoolbar.has_toolbar_folder", false);
user_pref("custtoolbar.personal_toolbar_folder", "");
user_pref("editor.author", "Michael Caloyannides");
user_pref("ghist.show_value", 1);
user_pref("ghist.sortby", -1);
```



AFTER CLEANING IT UP WITH WINDOW WASHER (OR MANUALLY)



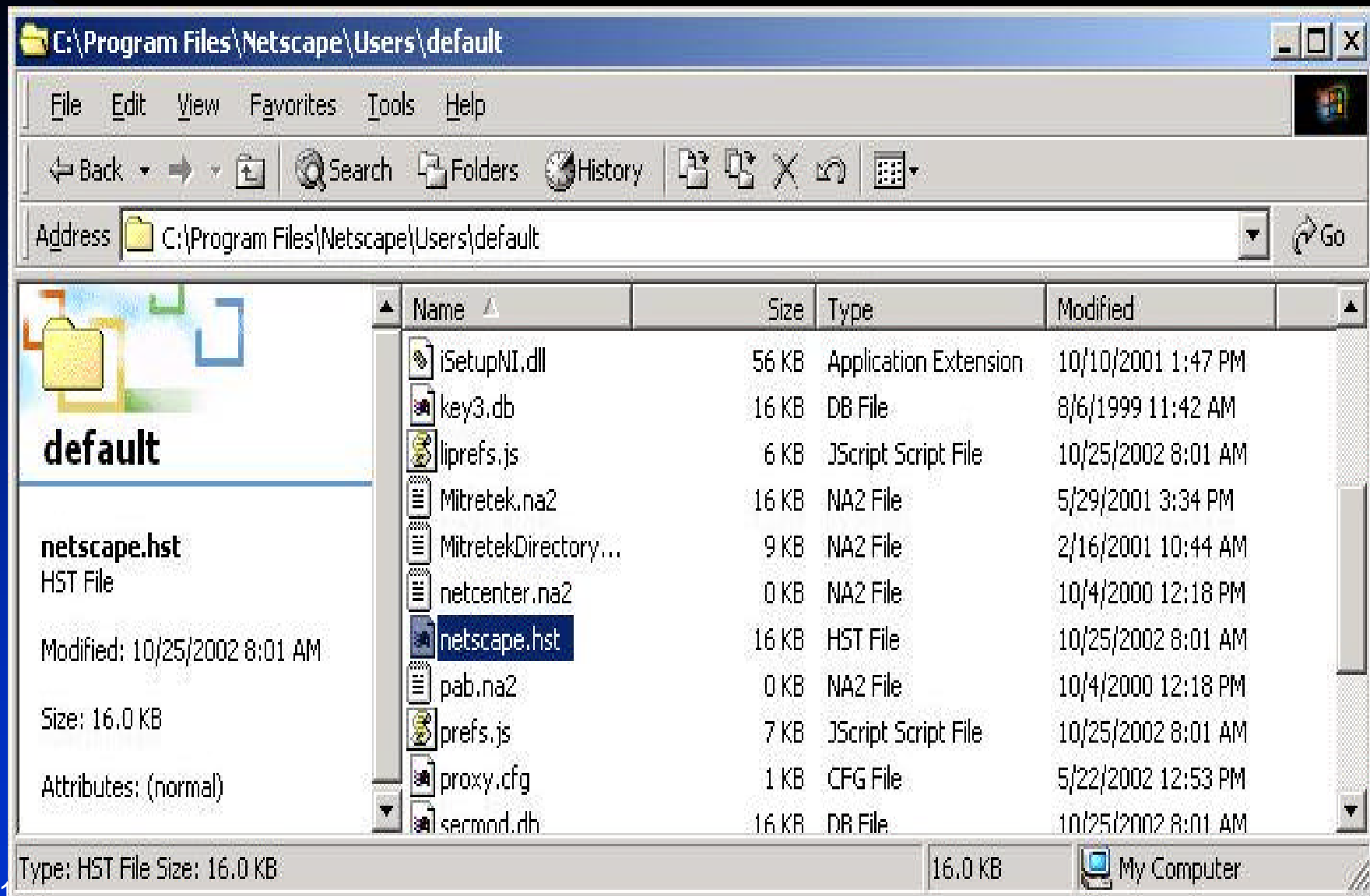
```
liprefs.js - Notepad
File Edit Format Help

// Netscape User Preferences
// This is a generated file! Do not edit.

user_pref("browser.enable_style_sheets", false);
user_pref("browser.link_expiration", 0);
user_pref("browser.startup.homepage", "http://internet.junkbuster.com/cgi-bin/show-proxy-args");
user_pref("browser.url_history.URL_0", "");
user_pref("browser.url_history.URL_1", "");
user_pref("browser.url_history.URL_2", "");
user_pref("browser.url_history.URL_3", "");
user_pref("browser.url_history.URL_4", "");
user_pref("browser.url_history.URL_5", "");
user_pref("browser.url_history.URL_6", "");
user_pref("browser.url_history.URL_7", "");
user_pref("browser.url_history.URL_8", "");
user_pref("browser.url_history.URL_9", "");
user_pref("browser.url_history.URL_10", "");
user_pref("browser.url_history.URL_11", "");
user_pref("browser.url_history.URL_12", "");
user_pref("browser.wfe.show_value", 3);
user_pref("custtoolbar.Messenger.Location_Toolbar.showing", false);
user_pref("custtoolbar.has_toolbar_folder", false);
user_pref("custtoolbar.personal_toolbar_folder", "");
user_pref("editor.author", "Michael Caloyannides");
user_pref("ghist.show_value", 1);
user_pref("ghist.sortby", -1);
```

AND THEN THERE IS "netscape.hst", too.

- ✗ It keeps a mildly encrypted running history of everything you have done with Netscape since day one.
- ✗ It has no socially redeeming value.
- ✗ It is NOT needed by Netscape to run.
- ✗ GET RID OF IT.
(But it a new one will be created)
- ✗ SO, KEEP GETTING RID OF IT.

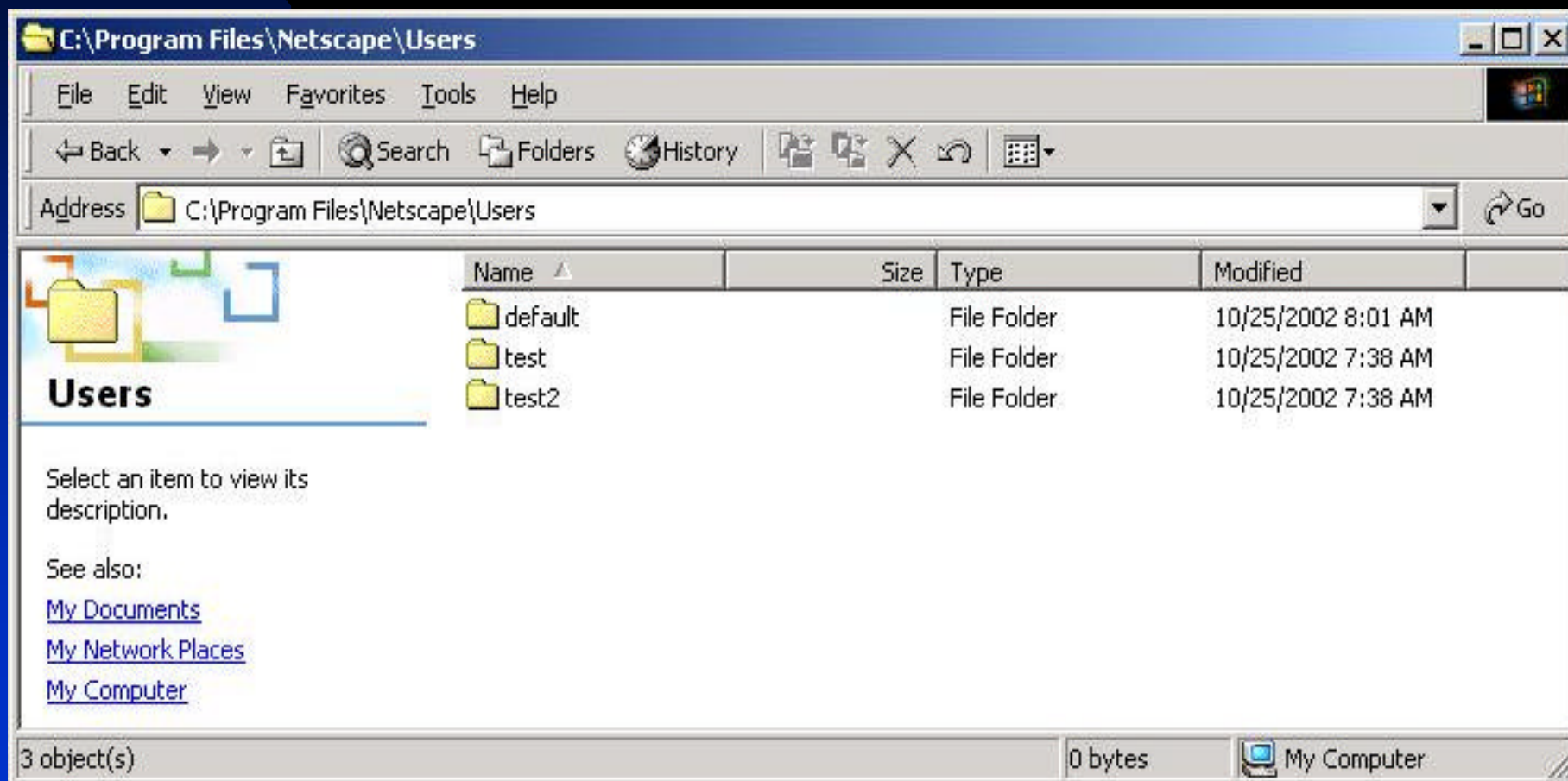


How to get rid of it for good?

1. **Overwrite** (NOT JUST DELETE) the existing netscape.hst in *C:\Program Files\Netscape\Users\Default*
2. Using a text editor, create a new file with nothing in it, call it “*netscape.txt*” and save it at that exact same folder location.
3. Rename *netscape.txt* into *netscape.hst*
4. Make it a “Read Only” file.
5. Periodically re-check it to make sure it has zero size.

(continued)

Do this for EVERY PROFILE you have in Netscape.



And then there are “cookies”...







- ✍ What are cookies?
 - ✍ The good
 - ✍ The bad and the ugly

(continued)

- ✍ How does one get rid of them:
 - ✍ Easier to refuse them in the first place
 - ✍ Better yet, accept them to fool the web site, but do not allow them to be written onto your hard disk.
 - ✍ There is a functionality penalty to be paid...

(continued)

For all browsers:

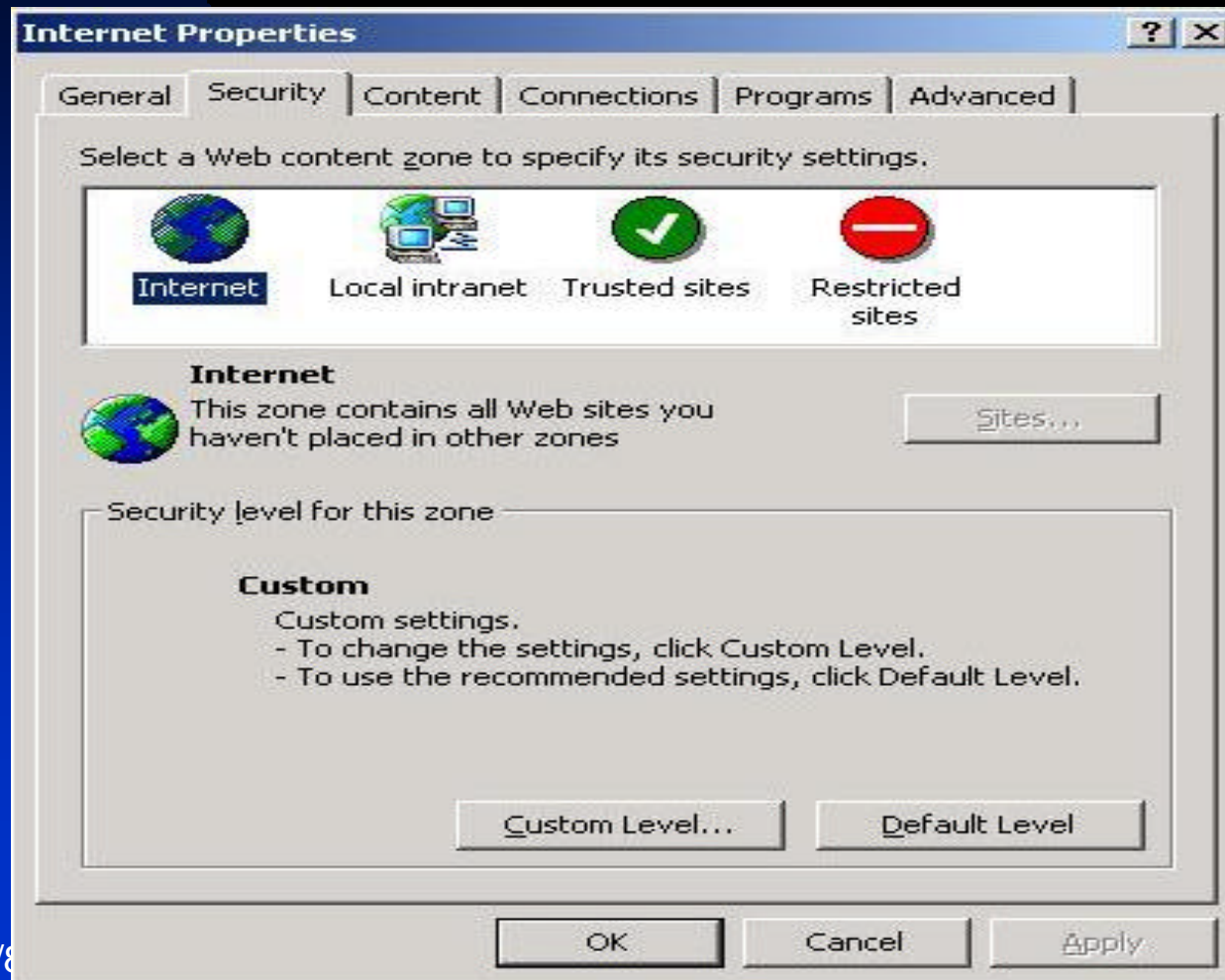
-  You can use any one of many cookie-limiting utilities available as freeware or shareware.
-  Consider using “junkbuster”; in addition to its normal function it also filters out cookies.
-  Consider using “NSClean” and “IEClean”
-  Consider using “WindowWasher”
-  Consider using “TrackEraser”
-  Better yet, use 2-3 of the above in cascade.

AND HOW ABOUT INTERNET EXPLORER?

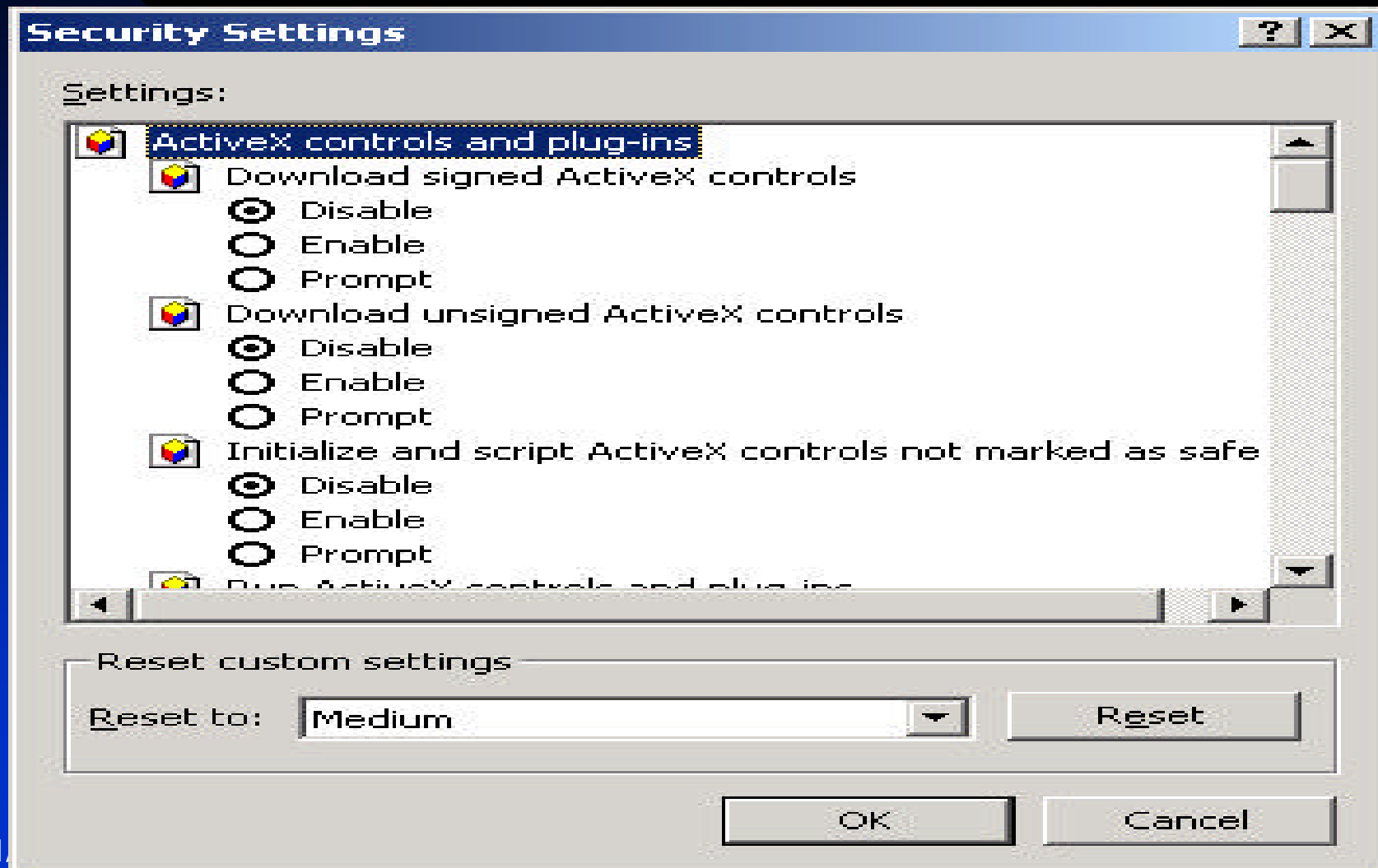
- ✍ If possible, don't use it, because:
 - ✍ It is far too integrated with the operating system.
 - ✍ It writes data about your online activities in the Registry which, if not cleaned carefully, can crash your computer.
 - ✍ There are multiple copies of the Registry in your computer; deleting the one you see in ResEdit does NOT affect the other copies.
- ✍ If you *still* want to use it, then do the following:

(continued)

- Start / Settings / Control Panel / Internet Options / Security
- Select "Custom"

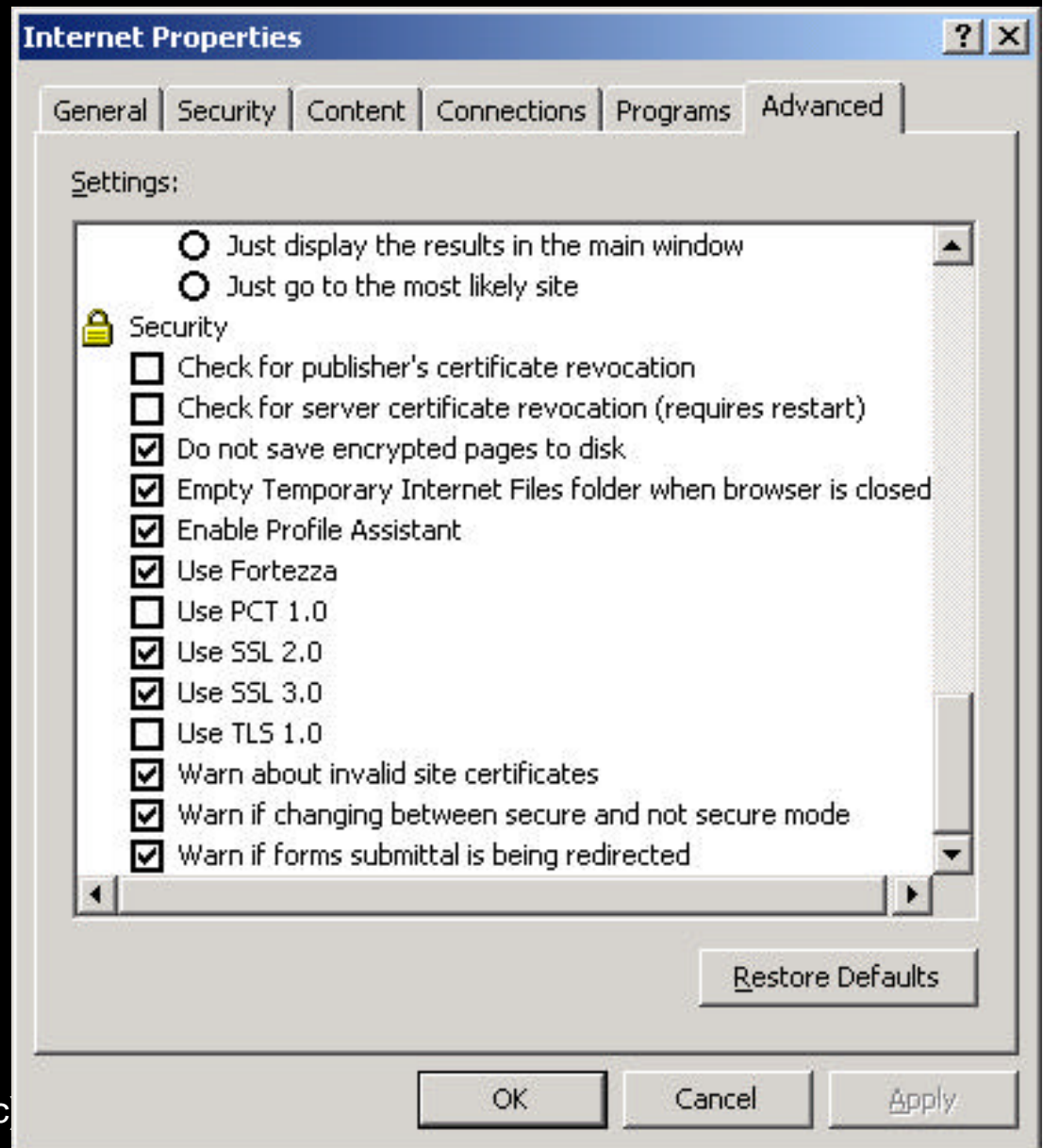


Set everything to "disable")



also:

- Start / Settings / Control Panel / Internet Options / Security
- Set things at the most conservative settings**



(continued)

➤ IN ADDITION: Download, install and use “SPIDER”

[Spider download page at WebAttack.com, delete/view IE index.dat ...](#)

... **Spider** 1.16 beta. delete/view **IE** index.dat file. ... **Spider** is a great tool for **privacy** concerned users, or can be used to reclaim disk space, since index.dat ...

[www.webattack.com/get/spider.shtml](#) - 20k - [Αποθηκευμένη Σελίδα](#) - [Παρόμοιες σελίδες](#)

[Another Reason for Spider-Man to Dislike Cookies](#)

... **IE** 6.0 uses the P3P standard to block or accept cookies based on the Web site's current **privacy** policy ... Cookies (read: **spider** webs) are even harder to get ...

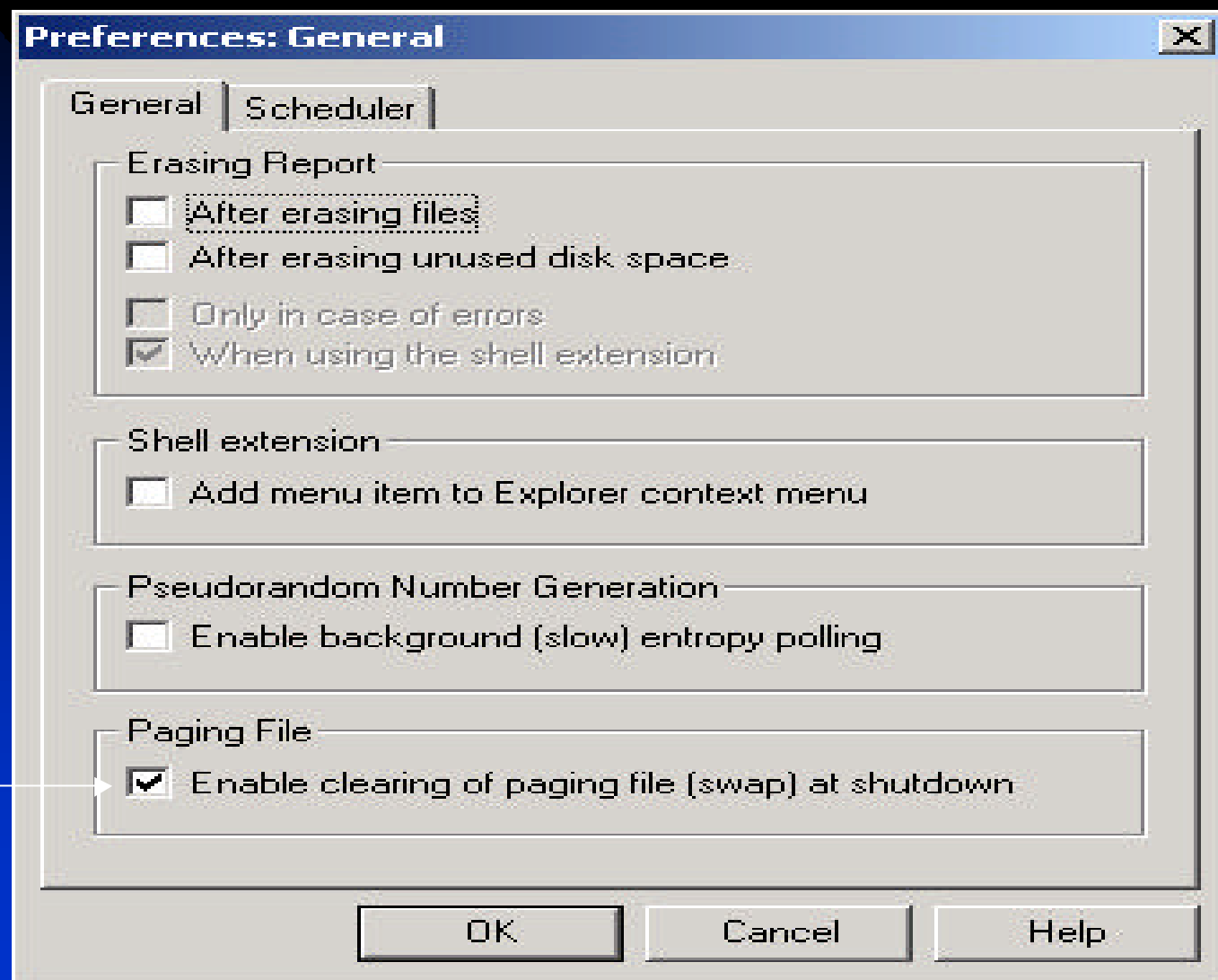
[www.clickz.com/aff_mkt/aff_mkt/print.php/1107321](#) - 10k - [Αποθηκευμένη Σελίδα](#) - [Παρόμοιες σελίδες](#)

In addition, regardless which web browser you use:

1. Remember to overwrite the caches...
2. Remember to overwrite the “swap” file...

You must overwrite both; consider using “Eraser”.
Yes, it takes a long time to overwrite a high capacity hard disk, but there is no choice.

Enable Windows' wiping of the swap file AFTER you set its (Virtual Memory's) size to a fixed value

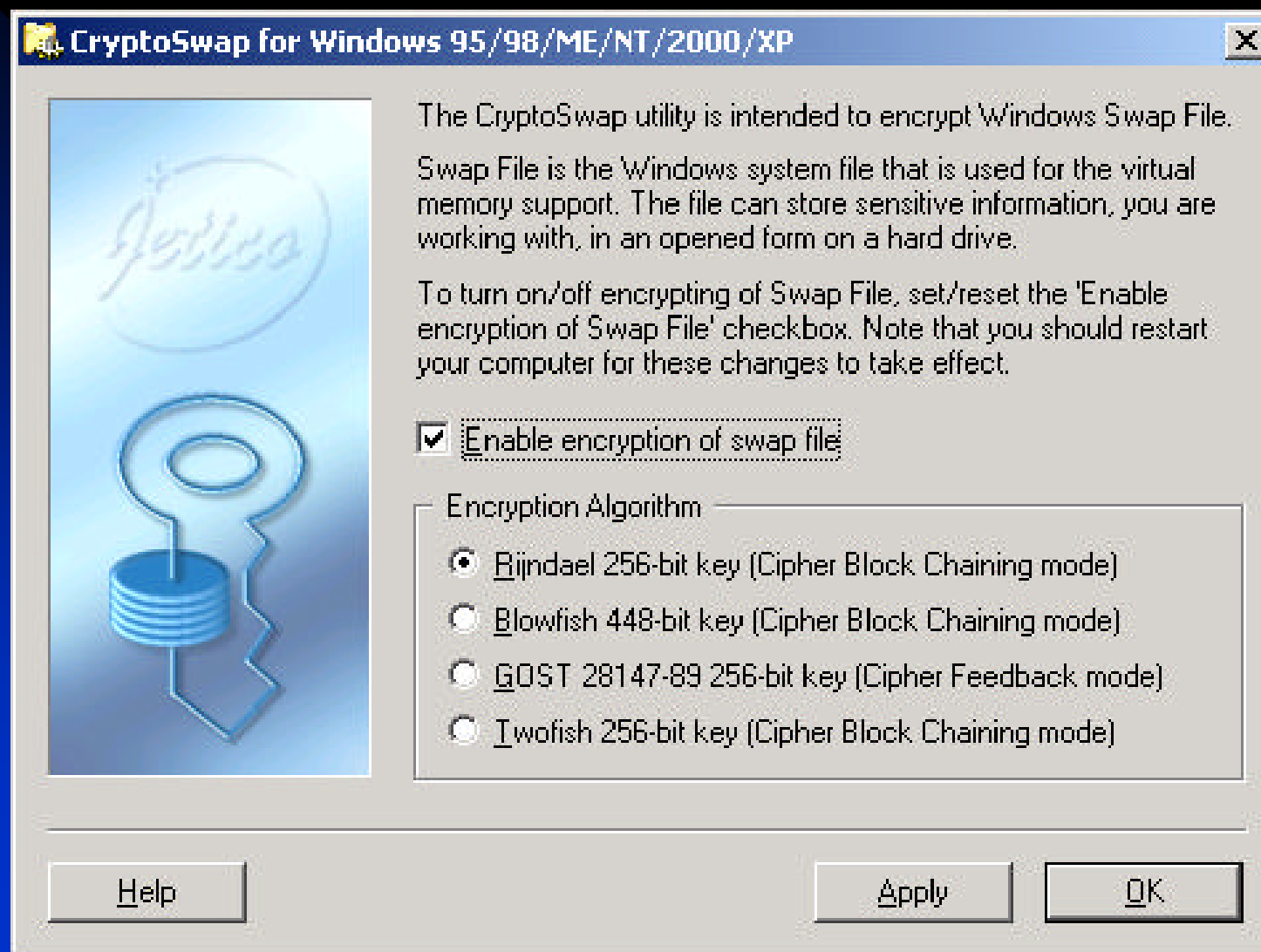


(continued)

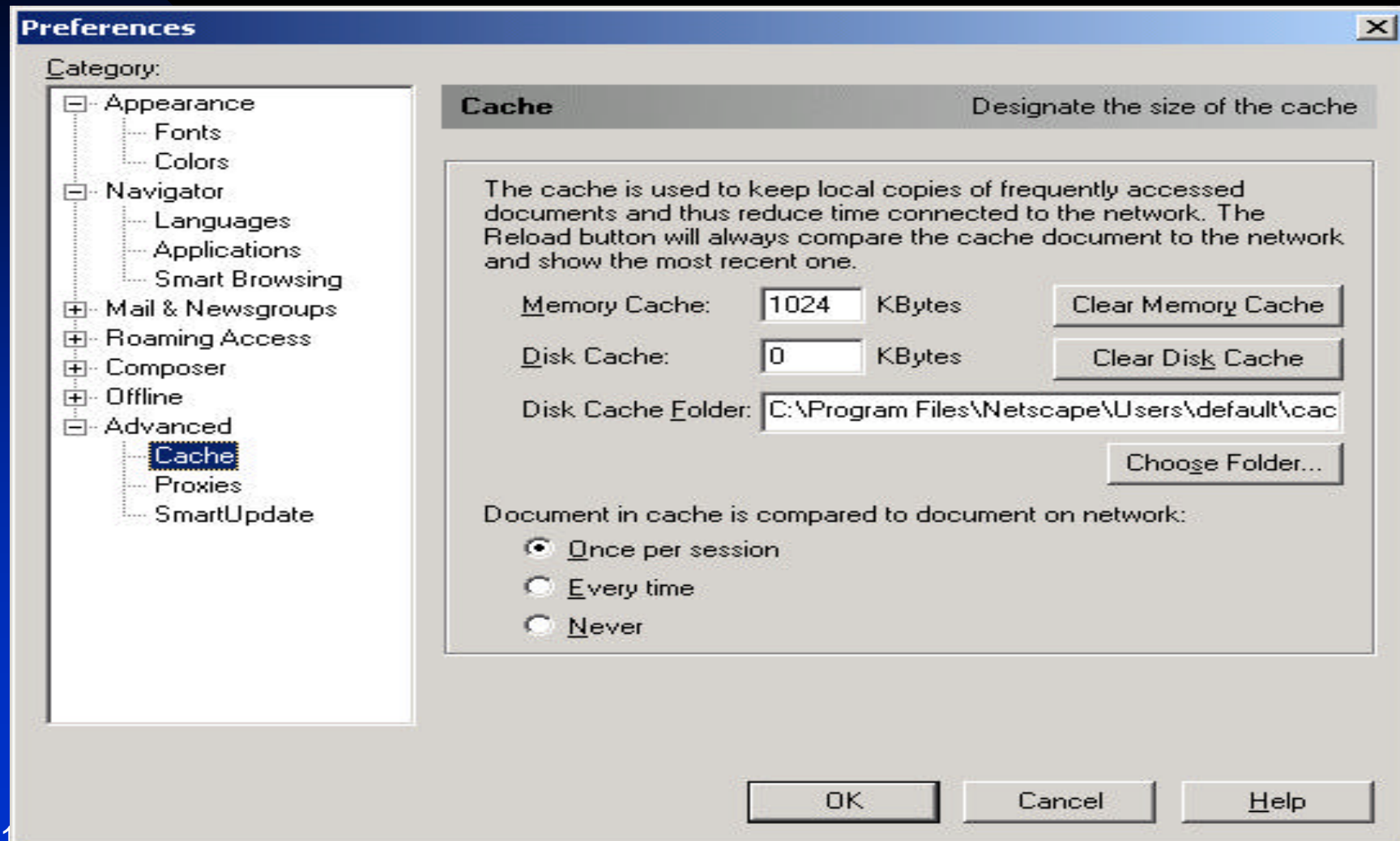
✍ As a bare minimum:

1. Disable all disk-caching in your web browser
2. Use “Best Crypt” to have a permanently encrypted swap file

(continued)



Set disk caching to zero



PROTECTING FROM WORTHLESS “PRIVACY POLICIES”

Worthless because:

- ✍ It can be (and often has been) changed by the company and is applied retroactively. The cases of amazon.com and Ebay are classical examples.
- ✍ Once a company goes bankrupt, its “confidential” list of customers and the data they provided to that company in confidence becomes just another “asset” that is sold to satisfy the bankrupt company’s creditors who, in turn, are not bound by the bankrupt company’s privacy policy.

Typically...

- ✍ On August 1, 2001, Essential.com, a company that retailed communications services, arranged to sell its customer list of 70,000 customers for \$1M and close down. That list was ostensibly protected by that company's "privacy policy".

http://www.boston.com/dailyglobe2/214/business/Essential_puts_on_fire_sale+.shtml

So, what do we do?

✍ The obvious:

- ✍ **Do NOT believe ANY privacy policy.**
- ✍ Assume any data you provide will end up in your worst enemies' hands; if that is ok with you, then provide the data. If not, don't.
- ✍ **Lie** if possible. (Perfectly legal unless under oath, intending to defraud, etc.).
 - ✍ Obviously not feasible in online orders
 - ✍ Perfectly feasible when exploring options in web sites.



IS THIS IT, THEN?

11/8/2002

(c) 2002 Michael Caloyannides

54

✍ No. All this protects you ONLY from a physical examination of your hard disk and ONLY partially; .

✍ **You have to worry separately about:**

1. Keystroke capturers in your computer (software or hardware)
2. Spyware in your computer
3. Web bugs of pages you access

(continued)

✍ And, of course, you also have to worry separately about:

1. Your ISP; he sees all. His records can be subpoenaed, too.
2. Telephone tap. (especially illegal ones)
3. The lack of discretion of the remote web sites you patronized

KEEP IN MIND THAT:

- ✍ Your computer can be analyzed **in your absence** from home/work.
- ✍ Your computer can be analyzed **remotely** while online.
- ✍ Your computer or hard disk(s) can be stolen or confiscated for later analysis.
- ✍ Off-site records are NOT magically untouchable!

THERE IS NO SILVER BULLET

- ✍ *“I want to be protected from disease; what single medicine should I take?”*
- ✍ Obviously no one preventive scheme can protect from all possible medical threats to one's health.
- ✍ Same in computer security.

COURTS ARE NOT DUMB...

- ✍ *“And would you tell the Court, sir, why you left your house in the rain to go use an Internet Café when you have a perfectly good computer and Internet connection at home?”*
- ✍ *“And would you tell the court why is it that you had a floppy disk with encryption software in your pocket when apprehended at the Internet Café that rainy night?”*

Investigators are not inept

- ✍ The State can avail itself of top notch expertise, lab facilities, etc.
- ✍ The State has limitless financial resources compared to you.

But protection is a lot of trouble...

- ✍ It is. So is the business of staying healthy.

- ✍ **But how painful to you would it be if:**

- ✍ Select snippets from everything you ever typed on the computer were presented out of context in a courtroom against you? (Civil or criminal)
- ✍ Select snippets of every web site you ever browsed were presented out of context in a courtroom against you?

(continued)

✍ **How painful to you would it be to you if:**

- ✍ Your business competitors got everything you ever typed on your computer (that you *think* you “deleted”?)
- ✍ A forensics examination of your computer that you bought used (or allowed someone else to use) found incriminating files that you never put there yourself?

PROTECTING FROM A REMOTE HACKER

- ✍ Start with a computer that has not been hacked into already.
- ✍ Install all existing security updates to the operating system software as well as to assorted applications software in it.
- ✍ Configure the computer to eliminate all *known* remaining vulnerabilities.

(continued)

- ✍ Install a current version of a good antivirus software and run it to ensure that the computer does not have a virus/Trojan/worm already.
- ✍ Install a good firewall and configure it in its most conservative setting. “*Zone Alarm Pro*” alone or in conjunction with either Black Ice or Norton’s “Internet Security” firewall or Signal 9’s “*Conseal*” is recommended.
- ✍ Install and run an “ad-ware” detection program. “Ad-aware” from lavasoft.de is recommended.

(continued)

- ✍ Install and run an application that will alert the user if a new program starts running in the background behind the user's back. "*WinPatrol*", "*Who's Watching*" and "*SpyCop*" are recommended for that purpose.
- ✍ If web-browsing is planned, install and use a local proxy program. "*Junkbuster*" is recommended. This requires some configuration of the web browser as well. Do not use "*Internet Explorer*" due to its use of ActiveX and the seemingly endless litany of security problems it has been associated with.
- ✍ For email, **avoid *Outlook* and *Outlook Express***; despite their conveniences, they have been associated with a vast number of serious security problems.

(continued)

- ✍ Never ever open email from a total stranger at all. Delete unread if it looks suspicious (e.g. “Subject: The Information You Requested”, when you never requested any, or from a sender that has an obviously fakes address).
- ✍ If the email had any attachments, do NOT EVER open those attachments. Find them and delete them unopened. Overwrite them if illegal.
- ✍ Open all email (from known senders) *after* going offline, never while you are still online; this is to negate “email web bugs”.

(continued)

- ✧ Most versions of Outlook and Outlook Express since 1997 do not check buffer overflows and allow a sender to execute arbitrary code of the sender's choice on the recipient's computer when the recipient opens the "vCard" sent by the sender.
- ✧ One could not configure either of these programs to ignore HTML code in incoming email. HTML is "cool" but grossly insecure.

PROTECTING FROM A BUSINESS COMPETITOR

- ✍ The case of the new VW employee from GM...
- ✍ The Lucent senior employee in 2001 and the Chinese...
- ✍ Impossible to protect entirely from a trusted employee.

YOU CAN HAVE SECURITY *OR* CONVENIENCE; **NOT BOTH**

- ✂ **Forget about Windows.** Go back to DOS

- ✂ >edit myfile.txt

- ✂ **Do NOT use a hard disk.** Floppies only. Have a two-floppy drive old fashioned system.

- ✂ Start with brand new clean floppies.

- ✂ Use a bulk eraser for good measure.

- ✂ **Use RAM-disk for all unencrypted text.**

- ✂ Save only encrypted text.

So, Who Does Computer Forensics?

- ✧ No official accreditation exists yet.
- ✧ An entire cottage industry has emerged to serve lawyers, law enforcers, employers, etc.
 - ✧ Small PDs can't afford their own.
 - ✧ Scarcity of defense lawyers who know which probing questions to ask...
- ✧ Universities are not graduating students in Information Security of forensics yet but the trend is changing:
 - ✧ Florida
 - ✧ Maryland
 - ✧ University of Tulsa

How Can That Data ("Evidence") Be Taken From Your Computer?

- ✍ 1) Direct physical access
- ✍ 2) Remote (online) access
- ✍ 3) Special techniques:
 - ✍ VanEck Radiation interception with commercial equipment & know-how.
 - ✍ Keystroke and/or screen capture
- ✍ 4) E-Mail forensics

Direct Physical Access

- ✍ Confiscation or on-site examination of computer or disks
- ✍ Confiscation of backup media
- ✍ Computer repair facility
- ✍ Physical entry during one's absence

[Direct Physical Access]

- ✍ Step 1: Make exact copy of target disk.
 - ✍ To prevent “evidence contamination”.
 - ✍ To defeat booby-trap software.
- ✍ Step 2: Analyze target disk.
 - ✍ Dispense with known commercial software
 - ✍ Look at history files, Registry, metadata, etc.
 - ✍ Look at “slack”, “empty space”
 - ✍ Look at unusual tracks/sectors
- ✍ Step 3: Piece evidence together.

[Direct Physical Access]

✂ The main software tools:

- ✂ “Encase”
- ✂ “FTK”
- ✂ “Expert Witness”
- ✂ Safeback
- ✂ FastSave
- ✂ Dd
- ✂ IPFilter
- ✂ DriveImagePro
- ✂ Norton Ghost
- ✂ Norton Disk Edit
- ✂ Anadisk
- ✂ Data Custodian
- ✂ The Coroner’s Toolkit (for Unix)

[Direct Physical Access]

✍ If no evidence can be found and there is still strong enough suspicion or political pressure:

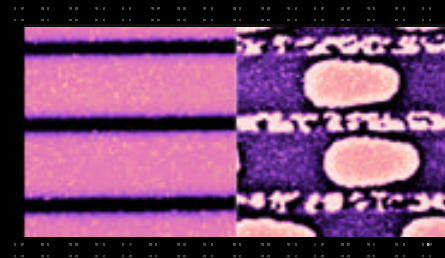
✍ Look for steganographically hidden data.

✍ Deploy Magnetic Forensic Microscopy.

[Direct Physical Access]

Magnetic Force Microscopy (MFM)

- ✍ Atomic resolution imaging
 - ✍ Example for magneto-optic media:



- ✍ Truly “deleting” data from magnetic media is near-impossible because of:
 - ✍ Imprecision of disk head positioning
 - ✍ Variability in media sensitivity & field strength over time.

[Direct Physical Access]

[Magnetic Force Microscopy (MFM)]

- ✍ In normal disks a logical “1” ends up being written as
 - ✍ ~ 1.05 when it overwrites a previous “1”
 - ✍ a ~ 0.95 when it overwrites a previous “0”.

It follows that, even with precise head alignment, one can read what was written before the last couple of overwritings.

[Direct Physical Access]

[Magnetic Force Microscopy (MFM)]

- ✍ DOD 5220.22-M prescribes 7 overwrites.
- ✍ Peter Gutman
(http://www.cs.auckland.ac.nz/~pgut001/secure_del.html) recommends 35 overwrites.
 - ✍ Even that may not erase the magnetic data because of the “defective sector handling problem”.

2) Remote (Online) Access




- ✗ Exploitation of any one of a vast number of web browser bugs.
- ✗ Exploitation of any one of many bugs of Outlook / Outlook Express or –to a far lesser extent- of other email software.
- ✗ Email attachment
- ✗ Installation of software by user (floppy disk, CD-ROM, etc.)
- ✗ LAN administrator access to employee's desktop is nearly limitless.
- ✗ Ad-ware / Spy-ware.
- ✗ “D.I.R.T.”
- ✗ etc., etc.

[Remote (Online) Access] – Ad-Ware

- A current list of reputed “ad-ware” is at <http://home.att.net/~willowbrookmill/spylist.pdf> <http://www.grc.com/>, <http://www.alphalink.com.au/~johnf/dspypdf.html>, <http://www.infoforce.qc.ca/spyware/>
- See alt.privacy.spyware for the latest
- An example: TSADBOT
 - Made multiple connections to CONDUCENT ad-servers.
 - Used proxy servers to defeat NETSTAT from finding actual addresses it connected to.
 - Could snoop web browser history and cache files.
 - Very hard to remove; stayed even after the ad-supported application that brought it in was removed.

[2) Remote (Online) Access] – Ad-Ware

FIXES:

-  Download and use “Ad-aware Plus” from <http://www.lavasoft.de>
-  Download and use Zone Alarm Pro to be alerted to outgoing communications attempts.
-  Manually search for known filenames of adware-affiliated files. (TSADBOT.exe, DSSAGENT.exe, adimage.dll, amcis.dll, anadsc.ocx, hetmdeng.exe, ipccclient.dll, msipcsv.dll, tfde.dll, tsad.dll, vcpdll.dll, flexactiv.dll, etc., etc.)


[2) Remote (Online) Access] – Ad-Ware


✍ FIXES (continued)

- ✍ Install and use a data analyzer for anything going out the modem (impractical)
- ✍ Look in STARTUP folder for new entries.
- ✍ **Do NOT use Netscape's "Smart Update"**
 - ✍ Legal case against it.
- ✍ **Do NOT use "registration wizards"**

[2) Remote (Online) Access] – Ad-Ware

FIXES (continued)

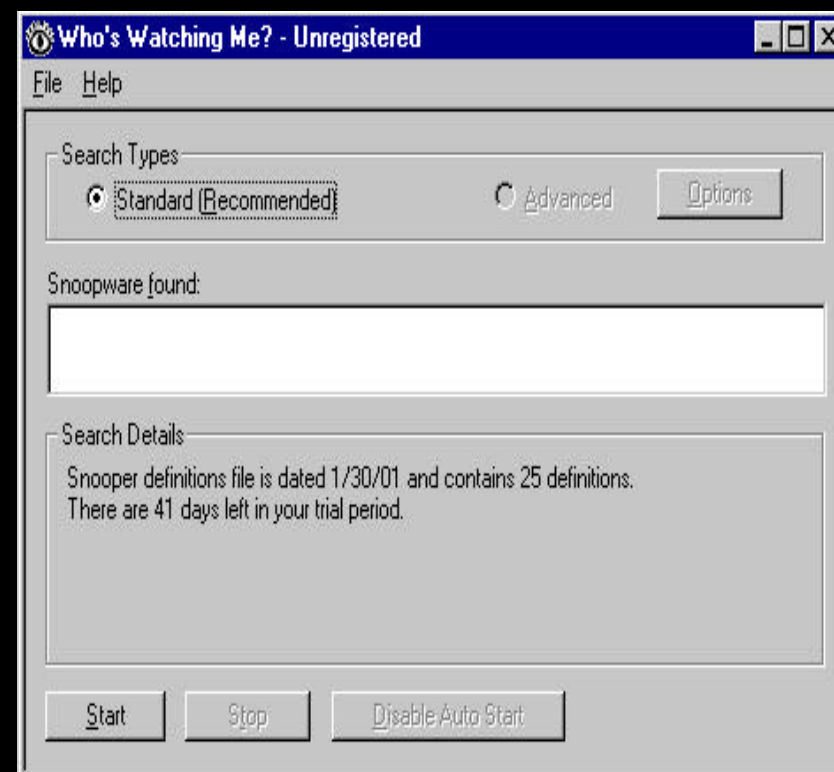
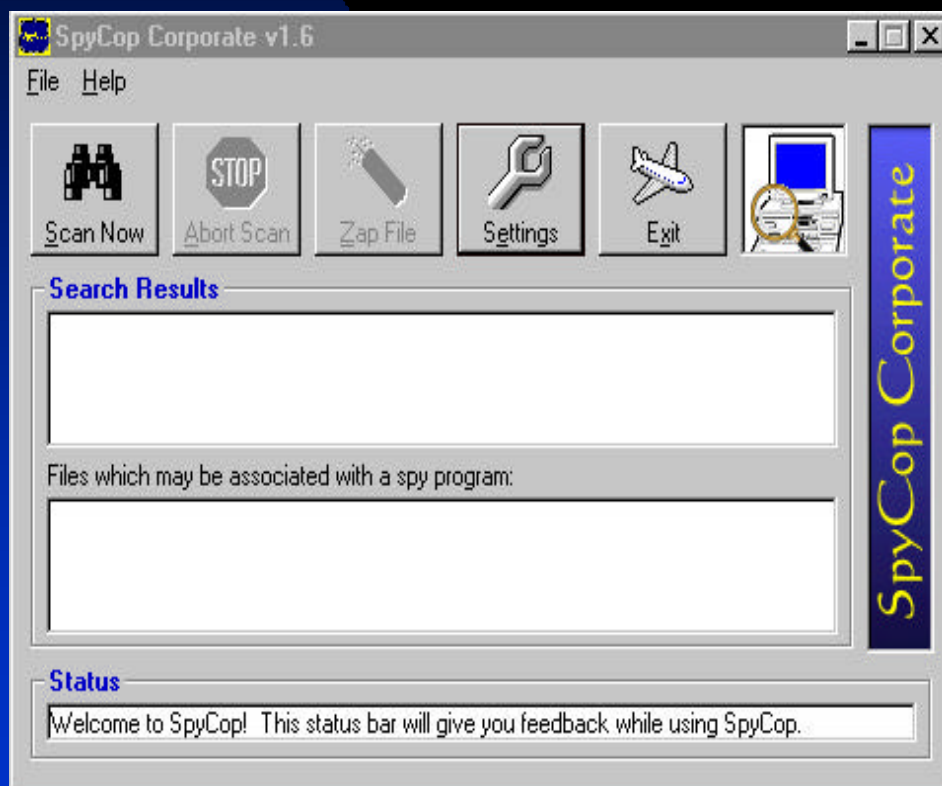
 **Disable “check for updates” features**
is various programs.

 E.g. in EUDORA, type: <x-eudora-
option:DontShowUpdates=1> into
message window. Hold down ALT key
and click on this URL; click OK to the
resulting question.

[Remote (Online) Access] – Ad-Ware

FIXES (continued)

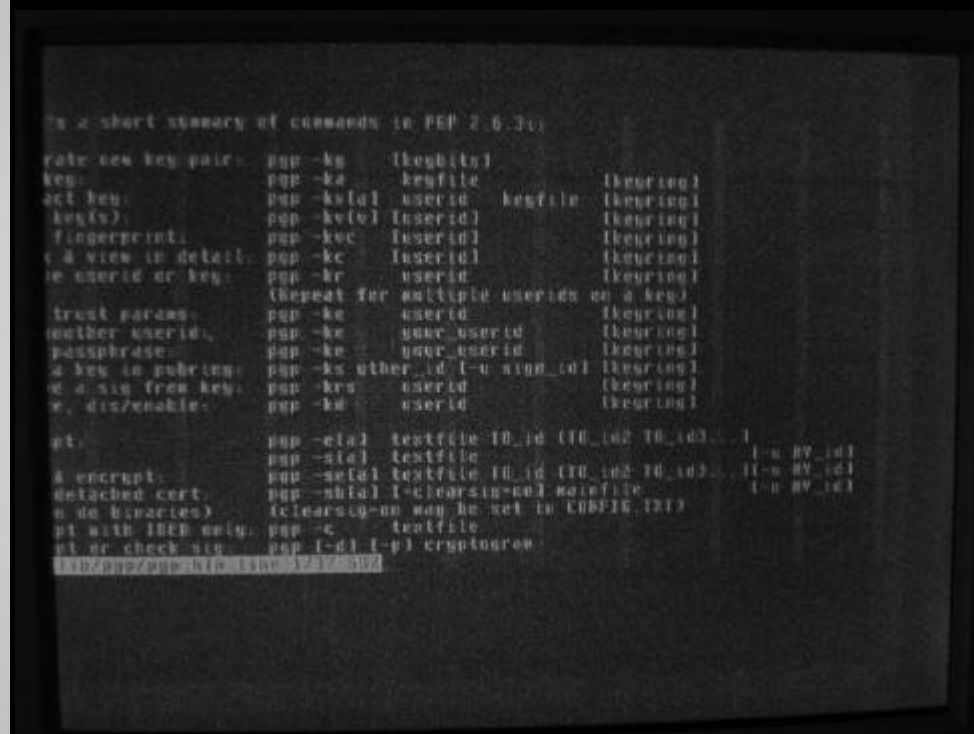
- Install and run assorted “spy-detect” software such as “SpyCop Corporate” (<http://www.spycop.com>) or “WhosWatching” (<http://www.trapware.com>), or “SpyDetect” (<http://www.spydetect.com>), etc.



3) Special Techniques

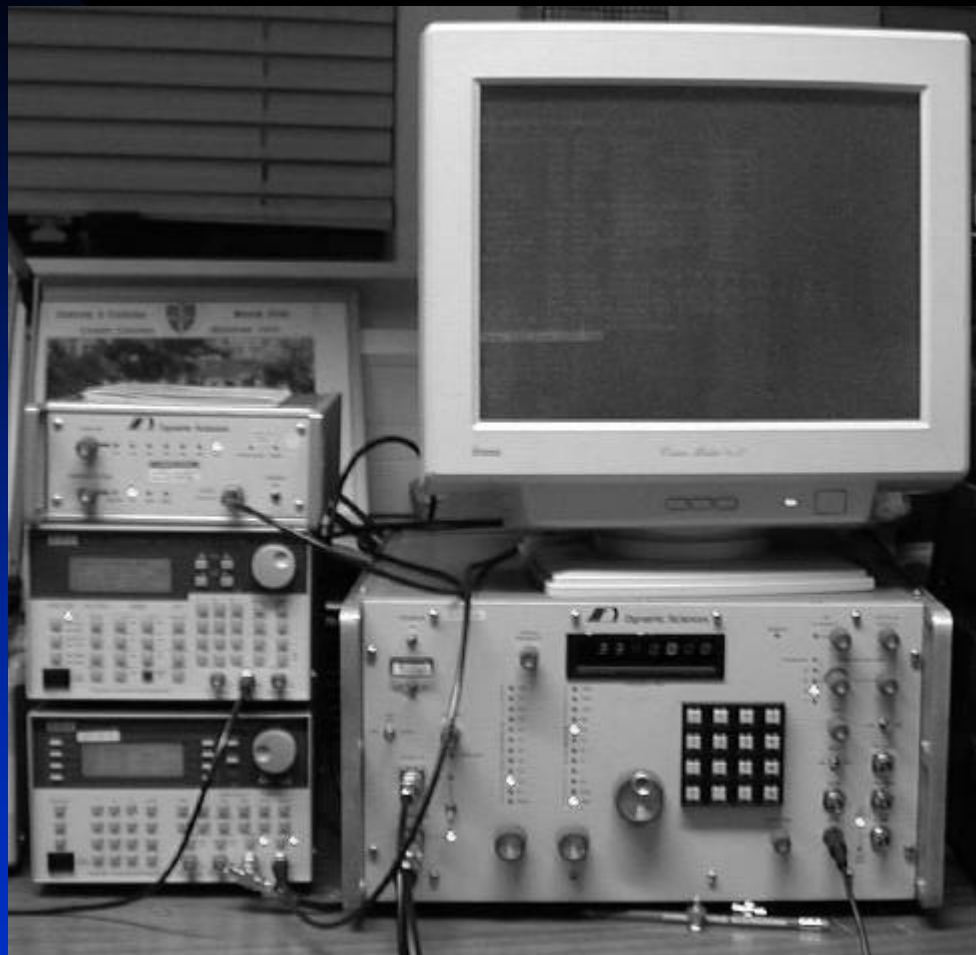
- ✍ Van Eck Radiation Interception **Using Openly Peddled Commercial Gear & Know-How**
- ✍ Keystroke-capturing and/or screen-capturing **commercially sold** software and hardware

[Special Techniques] – Van Eck



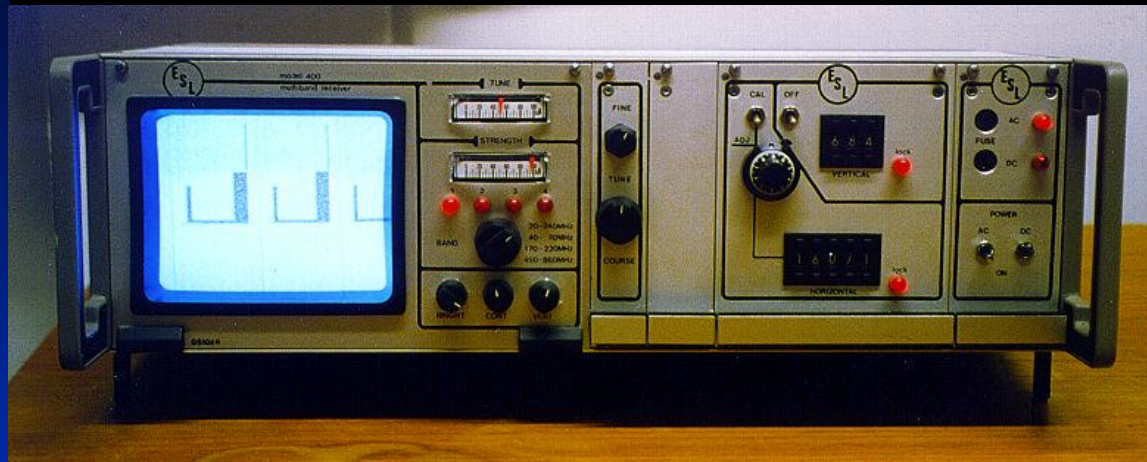
Hidden Data Transmission Using Electromagnetic Emanations”, University of Cambridge, Computer Laboratory, UK, available online at <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>):

[Special Techniques] – Van Eck



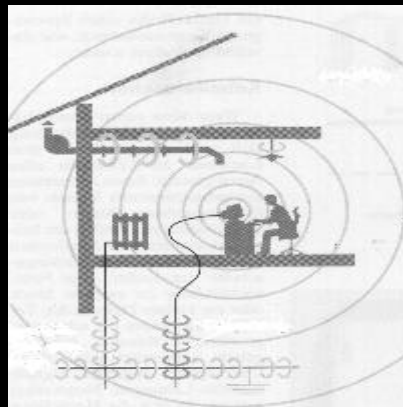
Courtesy of Kuhn and Anderson (“Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, University of Cambridge, Computer Laboratory, UK, available online at <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>):

[Special Techniques] – Van Eck



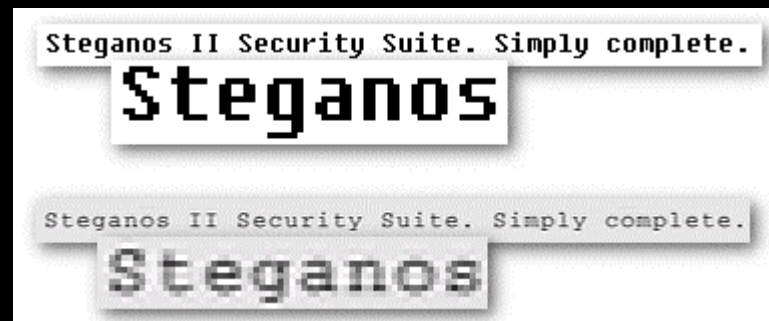
ESL Model 400 Commercial Equipment

[Special Techniques] – Van Eck



(<http://www.codexdatasystems.com/datascan.html>) to be usable for ranges **exceeding 1,000 yards**. (“The DataScan manufactured by CODEX captures the dominant video signal generated by any computer CRT screen and reconstructs it via a sophisticated antenna system and special receiver off-premises. Range has exceeded 1000 yards under optimum conditions. The unit is entirely passive in nature. It does not allow the user to access the target computer but rather to monitor via radio wave what is displayed on the target computers CRT screen every time the computer is operational.”)

[Special Techniques] – Van Eck



Partial commercial countermeasure
against interception of emanations.

[Special Techniques] – Keystroke Capturing



“Keyghost”, <http://www.keyghost.com>

[Special Techniques] – Keystroke Capturing

Model	Capacity	Ghost Playback	Encryption	Fast Download Adapter	Casing
<i>Keyghost II Professional SE</i>	2,000,000 Keystrokes	Yes	128 bit	Yes	EMC Balun
<i>Keyghost II Professional</i>	500,000 Keystrokes	Yes	128 bit	Yes	EMC Balun
<i>Keyghost II Standard</i>	97,000 Keystrokes	Yes	None	No	EMC Balun
<i>Keyghost Mini Covert</i>	120,000 Keystrokes	No	N/A	Yes	PS-2 Plug
<i>Keyghost II Security Keyboard (Pro)</i>	500,000 Keystrokes	Yes	128 bit	Yes	Keyboard
<i>Keyghost II Security Keyboard (Std)</i>	97,000 Keystrokes	Yes	None	No	Keyboard

“Keyghost”, <http://www.keyghost.com>

[Special Techniques] – Keystroke Capturing



“Keyghost”, <http://www.keyghost.com>

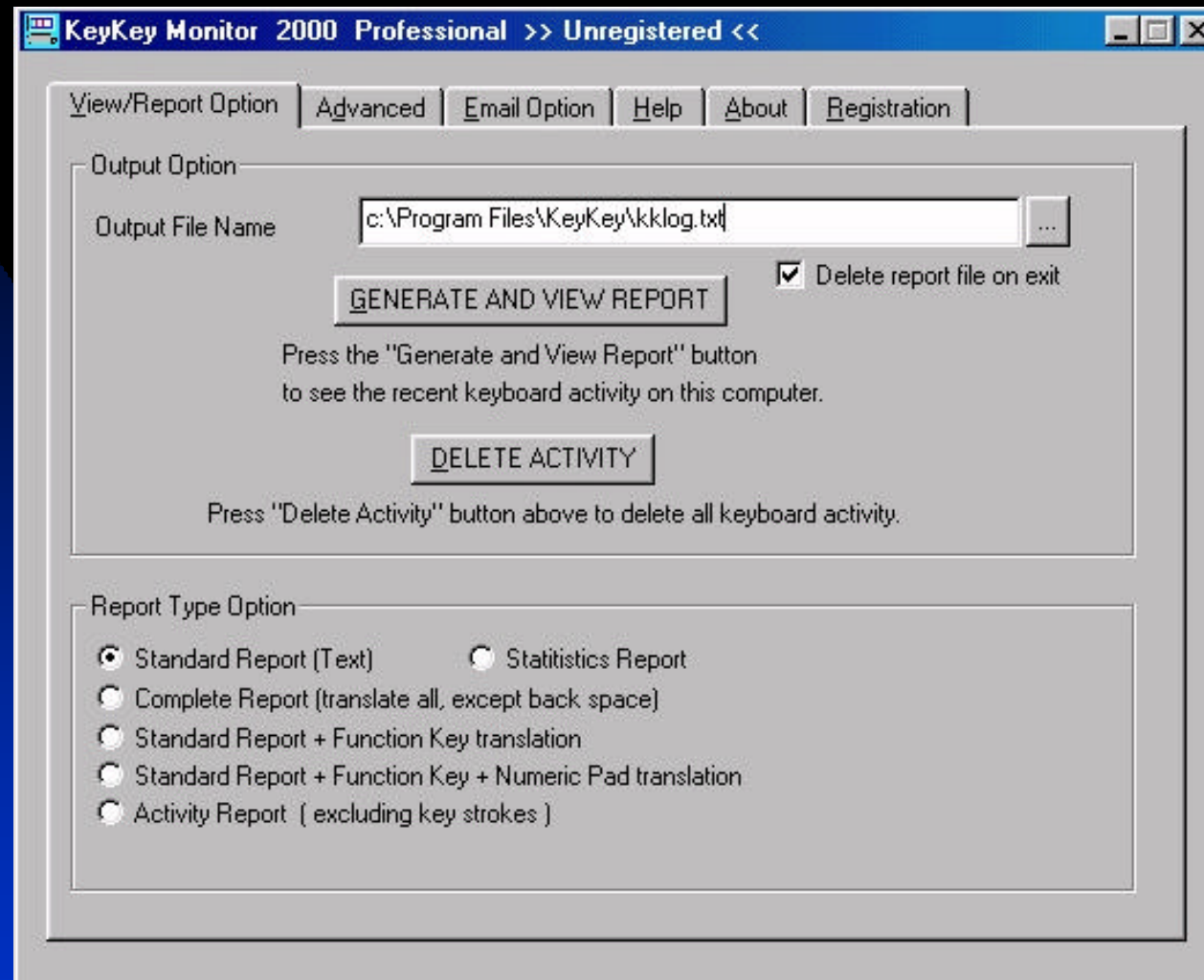
[Special Techniques] – Keystroke Capturing



“Keyghost” commercially sold device

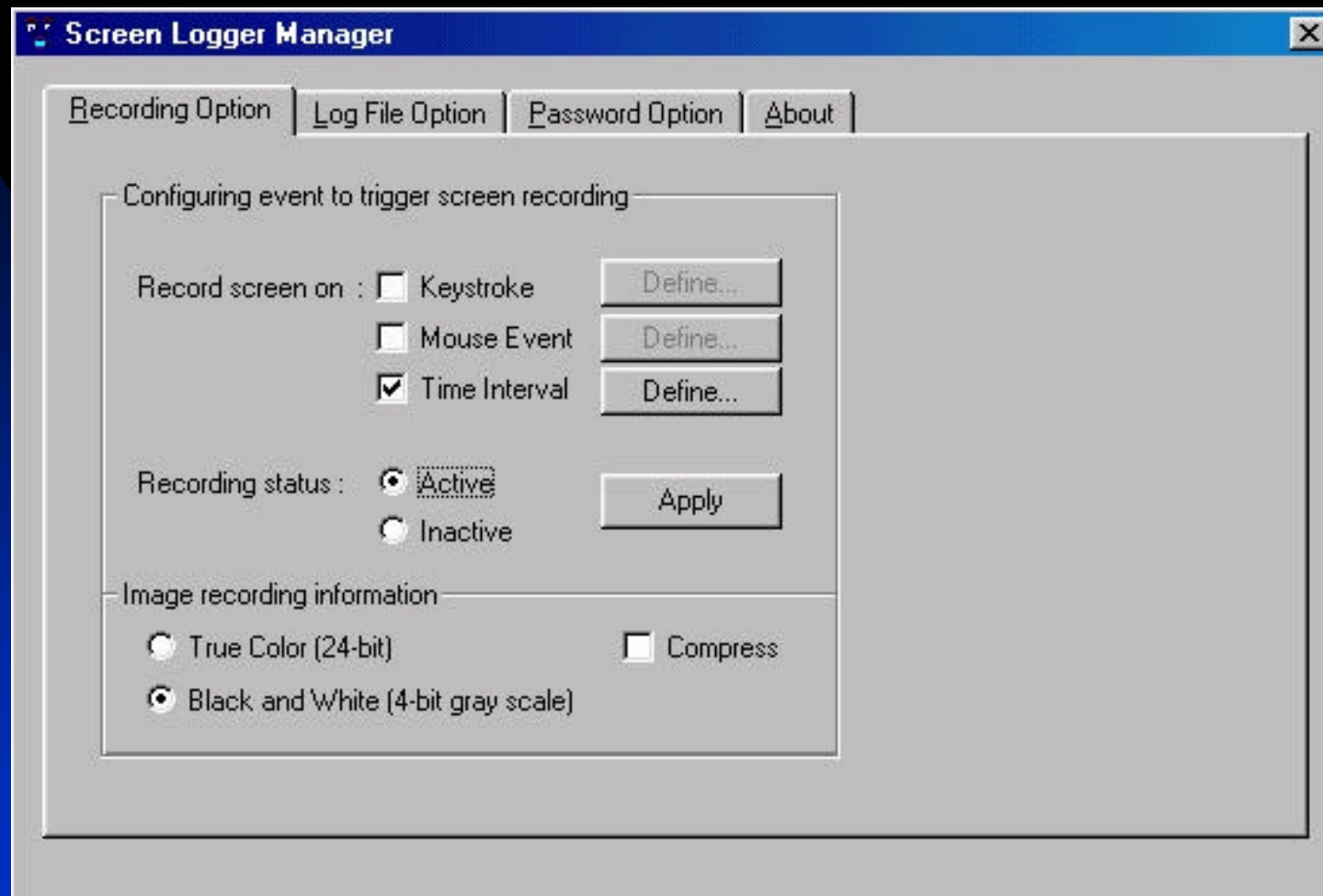


[Special Techniques] – Keystroke Capturing



“keykey” commercial software

[Special Techniques] – Keystroke Capturing



“keykey” commercial software

[Special Techniques] – Keystroke Capturing

Playback.zip

Win95pwgrabber.zip

Keycopy V.1.01

Keylogger V. 1.5

9x_int09.zip

achtung.zip

Internet Tracker

The Investigator

Gotyour Keystrokes

Spy Agent Professional

Net Spy

Desktop Detective

Spytech Shadow

Mom

“No Knock E-Warrant”

Raytheon’s “Silent Runner”

Keystroke capturing commercial software

[Special Techniques] – Keystroke Capturing

“D.I.R.T.” (Data Interception by Remote Transmission). This is a tool that claims to provide remote monitoring of one or more targeted computers **without the need for any physical access**. It is sold by Codex Data Systems (<http://www.codexdatasystems.com/menu.html>) .

According to that company’s own web site, “all that someone with DIRT needs to know is your email address. Period. All he has to do is send you an email with the imbedded DIRT-Trojan Horse and he is home free, and you are a clueless victim”.

4) Email forensics

- ✍ Faking outgoing email does not work.
 - ✍ Sender's software ads info to header
 - ✍ (message ID, email s/w, date/time)
 - ✍ ISP's SMTP server ads info to header
 - ✍ (real IP address of server, who the email came from, etc.)
 - ✍ Every node thereafter does likewise
 - ✍ (from which node, when, to which node)

Email forensics

From **fakedname@fakedISPname.com**
Fri Aug 18 12:27:43 -0400
Received: from **lastgobetween.com**
(lastgobetween.com [1.3.5.7])
by **recipientmailserver.com**
(2.4.5/2.4.5) with SMTP id DEF67890
for **recipient@recipientISP.com**; Fri.
18 Aug 2000 12:27:43 -0400

[Email forensics]

Expanded header format

Received: from *sending_server*
[(*sending_host_name*
sender's_IP_address)]
by *receiving_server* [(*software_version*)]
with *mail_protocol* and *id* [for
recipient_name]; *date*

[Email forensics]

Relay site format

Received: from relaysitename.com
(RELAYSITENAME.COM
[123.456.789.12])

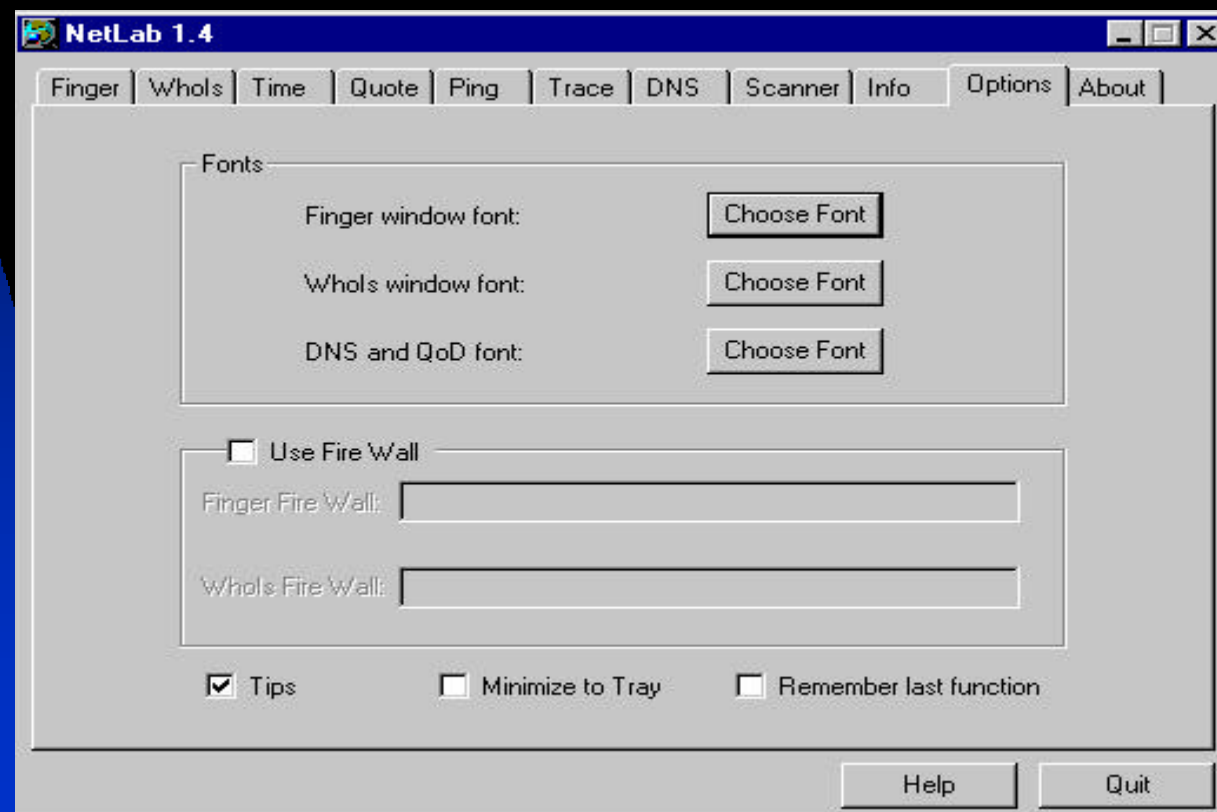
by receivingsite.com (1.2.3/1.2.3)
with SMTP if ABC12345

for recipientname@hisISP.com; Fri,
18 Aug 2000 12:22:41 -0400

[Email forensics]

Tracking suspect email

Numerous software packages, e.g.
NETLAB, etc.



[Email forensics]

Counter-countermeasures...

- ✍ **Anonymous remailers, proxies, etc.**
 - ✍ **Connection to them is detectable and matter of record.**
 - ✍ **Subsequent transaction may be hidden from SYSADMIN or local ISP if and only if the connection is encrypted.**

What This All Means

- ✍ Unless you use a computer with NO hard disk, **even the most advanced computer user will most likely leave traces behind that can be uncovered by computer forensics.**
- ✍ If you use a networked computer, even without a hard disk (unlikely), there will be additional forensic information at the ISP, employer's servers, etc., which will also record attempts to defeat forensics (e.g. anonymous remailers, encryption, etc.).

In short...

- ✍ In a perfect world, “if you have done nothing wrong, you have nothing to fear”.
- ✍ In the real world, recall Cardinal Richelieu’s words:
“Give me six lines written by the most honest man, and I will find something in them to hang him”.